Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1710 03/06/15

~ GOP Internet Freedom Act ~ People Are Talking! ~ EmuTOS Is Updated!
~ Huge Hacker Bust in U.K. ~ Hacker Wants PC Back! ~ Java Adware on Macs!
~ Open Letter to Atarians! ~ Jail for Facebook Post ~ Wolfenstein Prequel!

~ Schilling Shames Trolls! ~ New Beta of Mac OS X! ~ Heroes of the Dorm!

-* Facebook Reaches for Suicidal *-
-* Gaming's First Easter Egg: Adventure *-
-* Latest Web Security Bug May FREAK You Out! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

More snow, more cold - when will it all end??!! We have no more room for any more snow; and our tolerance of these frigid temperatures has quickly depleted! It's definitely been a record-breaking winter in more ways than one!

Very interesting issue this week. Net Neutrality isn't a done deal yet, if you can believe the news from the GOP. A new web security problem for internet users. Lots of interesting news for Mac users. Gaming news and interesting tidbits. Twitter trolls get their come-uppance, Major League style! And much, much more! So, rather then listen to me rail on about stuff this week, let's jump right in.

Until next time...

=~=~=~=

EmuTOS 0.9.4

Dear Atari users,

EmuTOS 0.9.4 has been released.

The main features are:

- Compile with -O2 by default for best optimization.
- New emutos-m548x-bas variant to support BaS_gcc on ColdFire Evaluation Boards.
- Less RAM usage: 94 kB saved from previous release.
- EmuDesk: Added feature to display text files.
- EmuDesk: Added feature to move files/folders with Control key.

You can download your preferred binary archive there:
http://sourceforge.net/projects/emutos/files/emutos/0.9.4/

Enjoy!

Vincent Rivière

Open Letter to Atari Users

The past year I have been registering shareware and donating to most of the software projects and sites that I frequently use under Windows, Mac, and Unix. I started wondering if there was a way an individual user can contribute easily to the Atari Software Community? I am talking about being able to donate to support Atari related Web Sites, Developers, etc. Very few sites have a Donate Button or an obvious way to donate some money to them. For example donating to ARANYM, AFROS, EmuTOS, FreeMiNT, SpareMiNT, Highwire, XaAES, Hatari, (add your other favorite Atari site or software here), etc.

Reason for me wondering is that I am aware that the number of Atari Enthusiasts and developers is dwindling as the years go on. Many if not all are doing it for the love of the platform, challenge, enjoyment and obviously not the money. Hosting Sites and bandwidth isn't free. Besides saying Thank You to the Developers and Site Administrators is to give them some money so that they can continue. Obviously none will be able to quit their day job but hopefully pay part if not all of their Hosting Fees and if lucky a few Dollars or Euros left over for a cup of coffee.

Over in the MorphOS Community (Amiga Clone OS) www.meta-morphos.org/ they have a couple of Support the Developer Donation Drives a year. The first drive in 2014 netted 41 Euros per developer (www.meta-morphos.org/viewtopic.php?topic=1294&forum=62). The second drive in 2014 netted 35 Euros per developer. On these drives the developer Opts In to the program and then splits the total raised equally among the developers in that fund raising drive.

This happens to work out real well for MorphOS because the Operating System is commercial and these are Independent Developers working on individual projects. For almost all the Atari related projects currently they are Open Source and in the example of FreeMiNT about a dozen active developers. If something along the lines of this type of program would be implemented in the Atari Community then possibly Project Web Sites can be included into the Donation Pool. Another option could be that Individual Developers and Site Administrators could be in the Donation Pool. Neither option is perfect. The first option helps support the Web Sites directly and the second option supports the individual developer and Admins who may or may not be working on multiple projects. Maybe an annual Drive for each method 6 months apart? I know that there are Software Bounties on other platforms but I don't recall ever seeing one for an Atari software project. Maybe this could be an option for very specific projects. I didn't even bring up the administrating of a project like this. That is whole other discussing.

I'm just throwing out my thoughts here if this is even possible to do in the community. The remaining Atari related sites and projects in my opinion are worth continuing. There must be a decent way to financially support our developers and sites. I will also post this question in a couple of Atari Forums for community discussion. If anybody has a better idea how we can Thank and Support our Atari Sites and Developers please comment on the forums.

=~=~=~=

->In This Week’s Gaming Section - Microsoft To Bridge Xbox and PC Video Gaming!

"""""""""""""""""""""""""""""""" Wolfenstein: The New Order Standalone Prequel
!

Gaming’s First Easter Egg - Adventure!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Microsoft Outlines Plan To Bridge Xbox and PC Video Gaming

Microsoft is attempting to break down the walls surrounding console gaming.

Phil Spencer, head of the company’s video game division, detailed Microsoft’s plan for game makers to create universal apps that can run on both Xbox One consoles and PCs with Windows 10, as well as smartphones, tablets and other devices running the forthcoming version of Windows. That includes HoloLens, Microsoft’s wearable headset that gives wearers the ability to interact with three-dimensional images.

"Our goal with gaming at Microsoft is to allow people to play games wherever they are," Spencer told game makers Wednesday at the Game Developers Conference. "We know for developers that it’s critically important for you to reach those gamers wherever they are."

Spencer said the marriage of Xbox One and Windows 10 would allow creators to make their games easily accessible to consumers, regardless of whether they switch between devices or where they buy apps.

"We know there are billions of people that play games across all devices," Spencer said. "Today, the world is segmented. You don’t have linkage really between the places that your customers are playing your games."

Microsoft Corp. first revealed its plans to bring Xbox and Windows closer together at the Jan. 21 unveiling of HoloLens and Windows 10, when Spencer demonstrated the upcoming Xbox One game "Fable Legends" running on a PC.

At the annual gathering of game developers on Wednesday, Spencer demonstrated the cross-play functionality on stage with a pair of players on Xbox One seamlessly facing off against another duo on PC in a match of the competitive multiplayer indie game "#IDARB."

Spencer also teased that Microsoft will release an adapter later this year that will allow PCs to use wireless Xbox One controllers. No price was announced.

In a private demo after Spencer's talk, Xbox director of program management Michael Ybarra showed off other functionality, including the abilities to record and edit game clips in Windows, find Xbox Live friends across multiple platforms and stream the Xbox One title "Sunset Overdrive" on a Microsoft Surface tablet.

Ybarra said game streaming will initially only be available on devices connected to the same network, but the company was looking into making it available across the Internet.

Microsoft is investing heavily in training developers on how to create games that work across its platforms this week by sponsoring such GDC sessions as "Developing with Xbox Live for Windows 10" and "Gaming Consumer Experience on Windows 10."

The move is part of Microsoft's bid to win back a larger audience after losing ground in the mobile computing boom. Windows has long been the dominant operating software for desktop and laptop computers, but business has suffered with more people using smartphones and tablets.

Wolfenstein: The New Order Standalone Prequel Announced

Bethesda on Wednesday announced Wolfenstein: The Old Blood, a standalone prequel to last year's critically acclaimed shooter Wolfenstein: The New Order.

The game, created by The New Order developer MachineGames, will launch on May 5 for $20. It will be available on that date for Xbox One, PlayStation 4, and PC through digital channels only.

The Old Blood, which is a two-part story, is set in 1946 when the Nazis are on the brink of winning World War II. You play as series hero B.J. Blazkowicz and embark on a perilous journey "deep within Bavaria."

Part One of The Old Blood is called Rudi Jäger and the Den of Wolves. B.J. faces off against a "maniacal prison warden" as he breaks into Castle Wolfenstein in an effort to steal the coordinates to General Deathhead's compound.

The Old Blood's second act, called The Dark Secrets of Helga Von Schabbs, sees B.J. venturing to the city of Wulfburg "where an obsessed Nazi archaeologist is exhuming mysterious artifacts that threaten to unleash a dark and ancient power."

The Old Blood also introduces new weapons, according to producer Jerk Gustafsson.

Diving back into the world of Wolfenstein has really been fun for us," Gustafsson said. We've enjoyed exploring the events leading up to The New Order. We think fans will really enjoy the story, all the action and, of course, jumping back into the combat with new weapons."

Additional gameplay for The Old Blood will be revealed during PAX East

this weekend in Boston.

The upcoming Old Blood standalone game might not be the last game MachineGames makes in the Wolfenstein series. Previously, the studio said, "We would love to do a sequel. We have a very, very clear idea of what we accomplished with this this, and what we want to accomplish with a sequel."

Blizzard Launches ’Heroes of the Dorm’ Tourney

Want to win free college tuition? Get out your game controller.

Blizzard on Friday announced a new Heroes of the Storm tournament for college students with more than $450,000 in tuition and prizes up for grabs. The so-called "Heroes of the Dorm" tourney is open to active college students in the U.S. and Canada and will have three rounds of competition.

Open qualifiers begin March 28, followed by a single-elimination bracket featuring 64 teams that starts on April 11. The event concludes with a final "Heroic Four" live event in late April. The final rounds of the tourney will be televised live on ESPN.

"Wrap up that term paper, because you’ll want to hit the Battlegrounds with no distractions," Blizzard wrote in its announcement.

Each team consists of five players. To enter, head over to the Heroes of the Dorm page and register your team by March 26. If you’re new to the game, no worries Blizzard will flag your account with beta access as soon as your team of five is registered and validated with a university email address.

Now, on to the most important information a breakdown of what you can win. All five members in the winning team will receive as much as $25,000 per year in college tuition for up to three years for their remaining undergrad or graduate enrollment. Seniors and grad students will receive one year’s worth of tuition to help repay student loans, or an equivalent cash prize for those lucky enough not to have any loans.

Each player whose team makes it to the Heroic Four will take home a "top-of-the-line gaming PC" featuring high-end components from Intel, Rosewill, CyberPower, and peripherals and accessories from SteelSeries and HyperX, as well as an all-expense paid trip to the finals in California.

Those not participating in the tournament can still get in on the action and compete for prizes in a Heroes of the Dorm fantasy bracket challenge, which kicks off April 3 when the top 64 teams are announced.

World of Warcraft Introduces Buying Game Time with Gold

Today, with a post on their website, Blizzard announced a new item will be making its way to World of Warcraft s real money e-shop relatively soon: the WoW Token. But what does said token do? Redeeming one in-game adds

30 days to the player s subscription. The important part of it all however, is that WoW tokens can be traded on the game s action house for in-game gold.

Essentially the idea is one player, tired of grinding for gold, but with more disposable income, purchases the token with real money. This player then sells it for in-game currency to someone who, while having a hoard of virtual gold, is a little strapped for the real kind, who then redeems it for the subscription extension.

This is not a new system in MMOs, having already been explored in other games, such as Eve Online, last year s Wildstar, and even further back in games like Second Life, to varying degrees of success. But this announcement marks the first appearance of a system of this kind, let alone a way to legally acquire gold with real-world money, in World of Warcraft.

Explaining the decision, Blizzard said:

We ve heard feedback from players that they d be interested in a secure, legitimate way to acquire gold that doesn t involve the use of unauthorized third-party gold-selling services one of the primary sources of account compromises. We also know players who ve amassed large amounts of gold through regular play would be interested in the ability to trade some to other players in exchange for game time, helping cover their subscription costs. The WoW Token feature gives players on both sides of the equation a secure and straightforward way to make that exchange. It opens up a new kind of payment option for World of Warcraft players, and we hope that it will also help lead to fewer account compromises and a better game experience overall.

As for pricing models and whether the WoW token will lessen gold-farming to the degree Blizzard is hoping, we will just have to wait and see. Last November the game s latest expansion, Warlords of Draenor, released, revitalizing the game.

EA Shuts Down SimCity Developer Maxis

EA has shut down Maxis Emeryville, the main Maxis studio and longrunning developer behind SimCity and Spore, among other games. Though the Maxis brand will carry on, the studio that most people knew as "Maxis" is no more.

"Today we are consolidating Maxis IP development to our studios in Redwood Shores, Salt Lake City, Helsinki and Melbourne locations as we close our Emeryville location," an EA representative said in a statement.

The news comes smack in the middle of the Game Developers Conference, where developers from across the world are congregating in San Francisco for various meetups, lectures, and sessions. It’s poor timing, to say the least.

I’ve been hearing rumblings about a shake-up at Maxis for a few days now, but official word first came this afternoon from former Maxis designer Guillaume Pierre, who wrote on Twitter this afternoon that the studio would be shutting down:

Later in the afternoon, EA confirmed plans to shut down Maxis Emeryville, sending over the following statement:

Today we are consolidating Maxis IP development to our studios in Redwood Shores, Salt Lake City, Helsinki and Melbourne locations as we close our Emeryville location. Maxis continues to support and develop new experiences for current Sims and SimCity players, while expanding our franchises to new platforms and developing new cross-platform IP.

These changes do not impact our plans for The Sims. Players will continue to see rich new experiences in The Sims 4, with our first expansion pack coming soon along with a full slate of additional updates and content in the pipeline. All employees impacted by the changes today will be given opportunities to explore other positions within the Maxis studios and throughout EA. For those that are leaving the company, we are working to ensure the best possible transition with separation packages and career assistance.

Originally founded in 1987, Maxis was best known for the Sim franchise, which began with Will Wright’s SimCity and expanded to include a number of other games, including the popular The Sims series, which is handled by a separate developer called The Sims Studio.

In 2013, Maxis released an online reboot of SimCity that was plagued with all sorts of problems, which may have been what led to this final closure. Neither SimCity nor the recent release of The Sims 4 performed very well, according to a person familiar with goings-on at the studio.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Gaming’s First Easter Egg - Adventure

It was 1979, and Atari programmer Warren Robinett was frustrated. The young engineer had already shipped a successful game called Slot Racers for the fledgling Atari 2600, and now he was working on something much more ambitious. Inspired by the text adventure games he d played on computer mainframes, Robinett was building Adventure, a fantasy-themed graphical exploratory game and the conceptual predecessor to the action RPG.

Opposed by his supervisor, Robinett worked on Adventure in secret. After delivering a proof of concept, he developed a groundbreaking console game with multiple rooms, interactive items, and a trio of deadly dragons each instilled with its own unique AI. Proud of his work, he wanted to add his signature to the game, but was blocked by his employer s corporate policies. Atari didn t allow software engineers to take credit for their games, fearing that if the identities of its most talented programmers were publicly known, they might be poached away by rival companies.

Robinett s solution was to create a hidden chamber in his sprawling map.

The tiny room was secreted in a maze and only accessible with a special item. Concealed within the room was a minuscule object, a single invisible pixel. By carrying that pixel into another area of the world and stacking two other items on the same screen, the player could render a certain wall passable. Stepping through the barrier led to yet another secret room. inside, the player would find the words Created by Warren Robinett.

Robinett left Atari soon after completing Adventure, and it wasn t until much later that his secret signature was discovered by a teenage player, who wrote Atari outlining his discovery. According to Robinett, Atari manager Steve Wright was amused by the inclusion of the hidden surprise, likening it to finding an Easter egg.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Republicans Internet Freedom Act Would Wipe Out Net Neutrality

US Rep. Marsha Blackburn (R-TN) this week filed legislation she calls the "Internet Freedom Act" to overturn the Federal Communications Commission’s new network neutrality rules.

The FCC’s neutrality rules prohibit Internet service providers from blocking or throttling Internet traffic, prohibit prioritization of traffic in exchange for payment, and require the ISPs to disclose network management practices.

These rules "shall have no force or effect, and the Commission may not reissue such rule in substantially the same form, or issue a new rule that is substantially the same as such rule, unless the reissued or new rule is specifically authorized by a law enacted after the date of the enactment of this Act," the Internet Freedom Act states.

Republicans in Congress already trying to overturn FCC s latest votes Comcast, AT&T, and Verizon are a bit miffed too.

The legislation has 19 cosponsors, Blackburn said in an announcement yesterday.

Once the federal government establishes a foothold into managing how Internet service providers run their networks they will essentially be deciding which content goes first, second, third, or not at all," Blackburn wrote. "My legislation will put the brakes on this FCC overreach and protect our innovators from these job-killing regulations.

In the latest election cycle, Blackburn received $25,000 from an AT&T political action committee (PAC), $20,000 from a Comcast PAC, $20,000 from a cable industry association PAC, and $15,000 from a Verizon PAC, according to the Center for Responsive Politics.

Blackburn’s legislation would also wipe out the FCC’s decision to reclassify broadband as a common carrier service subject to some of the Title II obligations imposed on wireline telephone and mobile voice. But while Internet providers and some Republicans have claimed to support net neutrality rules while opposing Title II reclassification, this bill would not leave any network neutrality rules in place. That’s not surprising, given that Blackburn has been trying to get rid of net neutrality rules for years.

Over the past year, Internet providers and Republicans have claimed that they are willing to accept the FCC enforcing net neutrality rules without a Title II classification, even though the FCC did just that in 2010 and still faced a lawsuit from Verizon. (Verizon won that lawsuit a year ago, forcing the FCC to reconsider how its net neutrality rules should be justified legally.) One Republican effort announced in January would enforce a version of net neutrality while gutting the FCC’s authority under Title II and Section 706, the latter of which was used by the FCC to preempt state laws that restrict municipal broadband projects. (Blackburn also filed legislation last week to overturn the municipal broadband decision.)

Blackburn’s Internet Freedom Act wouldn’t even enforce a weaker version of net neutrality, consistent with her past proposals. In 2011, she filed an "Internet Freedom Act" that would have struck down the FCC’s original net neutrality rules that were enforced without a Title II reclassification.

In February 2014, long before FCC Chairman Tom Wheeler decided to use Title II, Blackburn introduced another "Internet Freedom Act" that would have prohibited the FCC from issuing any new net neutrality rules.

Blackburn’s announcement yesterday notes that she "has been leading the fight against the Obama Administration s Net Neutrality regulations since they were first proposed in 2010 by Former Federal Communications Commission (FCC) Chairman Julius Genachowski." Blackburn is Vice Chair of the House Energy and Commerce Committee.

Rep. Fred Upton (R-Mich.) and Sen. John Thune (R-S.D.) have discussed legislation to overturn the FCC’s vote while keeping some version of net neutrality in place, but they haven’t finalized a bill yet.?"We don’t really have a Walden bill yet," said Rep. John Shimkus (R-Ill.), who cosponsored Blackburn’s legislation, Politico reported today. The Upton/Thune bill is "just theoretical," but the Blackburn bill at least has "some language to address what we think is a problem," Shimnkus said.

Upton, the House Energy & Commerce Chairman, told Politico that there are a lot of people who want a strong expression of opposition to the FCC s actions, and I expect [the Blackburn bill] will be one of many opportunities to weigh in."

The full text of the FCC’s net neutrality rules has not yet been finalized. They will take effect 60 days after publication in the Federal Register. FCC General Counsel Jon Sallet described the process in a blog post Monday.

Wheeler is expecting lawsuits, but he believes the commission’s latest rules rest on strong legal authority. The appeals court decision that overturned previous net neutrality rules faulted the FCC for imposing

per se common carrier obligations without classifying Internet providers as common carriers.

Classifying them as such "addresses that issue," Wheeler said last week.

Internet providers that today claim they would be happy with net neutrality rules that don’t rely on Title II are said to be "furious" with Verizon for challenging a weaker set of rules, allowing them to be replaced with stronger ones. AT&T hinted at that displeasure in a blog post that called the 2010 rules "a bipartisan win."

Back in 2010, AT&T said it preferred to avoid "government intervention" but also praised then FCC Chairman Julius Genachowski "for seeking a fair middle ground." At the time, AT&T said, "Today s vote, we trust, will put this issue behind us." But thanks to Verizon’s intervention, and legislation like Blackburn’s latest Internet Freedom Act, the net neutrality debate is far from over.

Twitter, Law Enforcement Investigate Alleged Islamic State Threats

Twitter Inc and law enforcement authorities are investigating alleged threats made by Islamic State militants against the social media network’s co-founder and other employees, the company said in reaction to media reports.

Islamic State supporters, in online posts on Sunday, called for attacks against Twitter and its "interests," including death threats, according to the online news media company Buzzfeed as well as the NBC news network.

"Our security team is investigating the veracity of these threats with relevant law enforcement officials," a representative for Twitter said in a statement on Monday. Buzzfeed first reported the story on Sunday.

One alleged threat was directed to Twitter co-founder Jack Dorsey, NBC reported. Dorsey didn’t address or acknowledge the threats in his latest tweets on Sunday.

The messages were posted on an anonymous file-sharing website called Pastebin, according to the media reports.

"Your virtual war on us will cause a real war on you, one post by Islamic State supporters said, according to Buzzfeed. "We told you from the beginning it’s not your war, but you didn’t get it and kept closing our accounts on Twitter, but we always come back."

Islamic State militants have relied heavily on Twitter and other social media networks to coordinate and to communicate, including the publishing of shocking videos of beheadings and other violent acts against its enemies.

But social media companies, including Twitter, have also removed content and suspended accounts that post gruesome content, such as executions.

Twitter’s user policy prohibits the use of the service for violence and threats, stating on its website: "You may not publish or post direct, specific threats of violence against others."

The company does not, however, "proactively monitor content," a spokesperson for the network told Reuters last week, adding that such policies were in place for other similar companies.

Twitter’s platform, which allows people to post 140-character messages with pictures and brief video clips, has more than 288 million users across the world, the company says.

Latest Web Security Bug Might FREAK You Out

Researchers this week disclosed a security flaw that has left some Apple and Google device users vulnerable to attack when visiting supposedly secure websites.

The vulnerability, known as FREAK (Factoring attack on RSA-EXPORT Key), dates back more than a decade, and opens those on the Android and Safari browsers to man-in-the-middle hacks when surfing various sites, including government pages.

According to the cryptographers who uncovered the flaw, "Freak" targets deliberately weak export cipher suites, which were introduced "under the pressure of U.S. governments agencies to ensure that the NSA would be able to decrypt all foreign encrypted communication."

Support for most of these algorithms are disabled by default, but there is a loophole, the researchers said.

"If a server is willing to negotiate an export ciphersuite, a man-in-the-middle may trick a browser (which normally doesn’t allow it) to use a weak export key," their website said.

Many U.S. government agencies (NSA, FBI) and other popular sites (IBM, Symantec) enable those export ciphersuites on their servers, allowing hackers to impersonate them to vulnerable clients.

Folks using Chrome, Firefox, or Internet Explorer to connect to sites offering strong ciphers are probably not affected, the team said. But anyone running a browser with a buggy TLS library, over an insecure network, connecting to an HTTPS server with export ciphersuites, may be vulnerable.

Check out an abridged list of insecure sites including American Express, Bloomberg, National Geographic, Cornell University, and the Ohio government, among others; the full lineup of domains is also available online.

Web administrators can use the SSL Labs’ server test to check their site’s risk level. If vulnerable, they should disable support for all known insecure ciphers and enable forward secrecy.

An Apple spokesman told PCMag that an iOS and OS X fix will be pushed out next week.

Google, meanwhile, is currently providing a patch to partners, Reuters reported. The company did not immediately respond to PC Mag’s request for comment.

Microsoft Warns Windows PCs Also Vulnerable to ’Freak’ Attacks

Hundreds of millions of Windows PC users are vulnerable to attacks exploiting the recently uncovered "Freak" security vulnerability, which was initially believed to only threaten mobile devices and Mac computers, Microsoft Corp warned.

News of the vulnerability surfaced on Tuesday when a group of nine security experts disclosed that ubiquitous Internet encryption technology could make devices running Apple Inc’s iOS and Mac operating systems, along with Google Inc’s Android browser vulnerable to cyberattacks.

Microsoft released a security advisory on Thursday warning customers that their PCs were also vulnerable to the "Freak" vulnerability.

The weakness could allow attacks on PCs that connect with Web servers configured to use encryption technology intentionally weakened to comply with U.S. government regulations banning exports of the strongest encryption.

If hackers are successful, they could spy on communications as well as infect PCs with malicious software, the researchers who uncovered the threat said on Tuesday.

The Washington Post on Tuesday reported that whitehouse.gov and fbi.gov were among the sites vulnerable to these attacks, but that the government had secured them.

Security experts said the vulnerability was relatively difficult to exploit because hackers would need to use hours of computer time to crack the encryption before launching an attack.

"I don’t think this is a terribly big issue, but only because you have to have many ducks in a row," said Ivan Ristic, director of engineering for cybersecurity firm Qualys Inc.

That includes finding a vulnerable web server, breaking the key, finding a vulnerable PC or mobile device, then gaining access to that device.

Microsoft advised system administrators to employ a workaround to disable settings on Windows servers that allow use of the weaker encryption. It said it was investigating the threat and had not yet developed a security update that would automatically protect Windows PC users from the threat.

Apple said it had developed a software update to address the vulnerability, which would be pushed out to customers next week.

Google said it had also developed a patch, which it provided to partners that make and distribute Android devices.

"Freak" stands for Factoring RSA-EXPORT Keys.

’FREAK’ New SSL/TLS Vulnerability Explained

Another new widespread and disastrous SSL/TLS vulnerability has been uncovered that for over a decade left Millions of users of Apple and Android devices vulnerable to man-in-the-middle attacks on encrypted traffic when they visited supposedly ’secured’ websites, including the official websites of the White House, FBI and National Security Agency.

Dubbed the "FREAK" vulnerability (CVE-2015-0204) - also known as Factoring Attack on RSA-EXPORT Keys - enables hackers or intelligence agencies to force clients to use older, weaker encryption i.e. also known as the export-grade key or 512-bit RSA keys.

FREAK vulnerability discovered by security researchers of French Institute for Research in Computer Science and Automation (Inria) and Microsoft, resides in OpenSSL versions 1.01k and earlier, and Apple’s Secure Transport.

Back in 1990s, the US government attempted to regulate the export of products utilizing "strong" encryption and devices were loaded with weaker "export-grade" encryption before being shipped out of the country.

At that time, it was allowed a maximum key length of 512 bits for "export-grade" encryption. Later in 2000, with the modification of the US export laws, vendors were able to include 128-bit ciphers in their products and were able to distribute these all over the world.

The only problem is that "export-grade" cryptography support was never removed and now three decades later, FREAK vulnerability make it significantly easier for hackers to decode the website s private key and decrypt passwords, login cookies, and other sensitive information from HTTPS connections.

Assistant Research Professor Matthew Green of Johns Hopkins University’s Information Security Institute in Maryland summarizes the FREAK vulnerability in a blog post detailing how a hacker could perform MitM attack:

In the client’s Hello message, it asks for a standard ’RSA’ ciphersuite.
The MITM attacker changes this message to ask for ’export RSA’.
The server responds with a 512-bit export RSA key, signed with its long-term key.
The client accepts this weak key due to the OpenSSL/Secure Transport bug.
The attacker factors the RSA modulus to recover the corresponding RSA decryption key.
When the client encrypts the ’pre-master secret’ to the server, the attacker can now decrypt it to recover the TLS ’master secret’.
From here on out, the attacker sees plain text and can inject anything it wants.

A scan of more than 14 million websites that support the SSL/TLS protocols found that more than 36% of them were vulnerable to the decryption attacks that support RSA export cipher suites (e.g., TLS_RSA_EXPORT_WITH_DES40_CBC_SHA).

Cracking a 512-bit key back in the ’90s would have required access to supercomputers of that time, but today, it can be done in seven hours and cost nearly $100 per website only.

It is possible to carry out FREAK vulnerability attack when a user running a vulnerable device currently includes Android smartphones, iPhones and Macs running Apple's OS X operating system connects to a vulnerable HTTPS-protected website. At the moment, Windows and Linux end-user devices were not believed to be affected.

FREAK vulnerability is similar to last year's POODLE flaw or Padding Oracle On Downgraded Legacy Encryption, which allowed hackers to downgrade the entire SSL/TLS Internet-communication security suite to the weakest possible version. FREAK affects only those SSL/TLS implementations that accept export versions of protocols that use the RSA encryption algorithm.

Security researchers are maintaining a list of top vulnerable websites and encourage web server administrators to disable support for export suites, including all known insecure ciphers, and enable forward secrecy.

You can also use an Online SSL FREAK Testing Tool to check whether a website is vulnerable or not.

Google said an Android patch has already been distributed to partners. Meanwhile, Google is also calling on all websites to disable support for export certificates.

Apple also responded to the FREAK vulnerability and released a statement that, "We have a fix in iOS and OS X that will be available in software updates next week."

Alleged US Army Hacker Lauri Love Wants His Computers Back

A British man arrested on suspicion of hacking into the computer systems of the United States Army and other federal agencies is petitioning for the return of his encrypted computers and storage devices.

Lauri Love was arrested in October 2013 following a joint investigation by the US Army's criminal investigation command and the FBI in Newark.

Now Love wants computer equipment seized at the time of his arrest returned.

According to the BBC, the UK's National Crime Agency (NCA) doesn't want to give up the equipment because it has been unable to decrypt some of Love's files. It allegedly wants Love's cooperation in helping to decrypt them before returning his property.

Speaking to the BBC, Love said:

Should police, having obtained a reason to acquire information but lacking any overt evidence of criminality sufficient to bring prosecution, be allowed to withhold private data?

There is a very dire risk that this power will be used to disrupt protected journalistic and political activity.

Love later contacted Ars Technica to say he had submitted his petition to the court earlier this month and would be representing himself at a

hearing on the 12 March. He added:

I cannot speak to the contents except that they are mine.

This is the only salient detail as far as I'm concerned. I am not on trial, nor is my data, and I am under no obligation to speak for it. But my property is being withheld from me, and that must be justified.

The current justification is due to the inability of the NCA to understand certain data. It remains for them to establish why this is my problem and for the court to decide if this gives them authority to convert chattel.

The agency has declined to reveal whether it has been unable to decrypt Love's files.

Love, who stands accused of working with three other unnamed people, faces charges of breaching the security of the US military, NASA, the Environmental Protection Agency, US Federal Reserve and FBI computers.

Other charges including computer hacking and identity theft leave him facing a sentence of up to 12 years in prison if convicted but the fact that the NCA released him from bail back in July would seem to suggest that any case for the prosecution may rely upon gaining access to the encrypted files currently in the agency's possession.

The US may yet seek to extradite Love after a 2013 US Department of Energy audit suggested he may have gathered personal information on as many as 104,000 people.

Co-creator of Blackshades Malware Used To Spy on Miss Teen USA Pleads Guilty

One of the co-creators of the Blackshades Remote Access Trojan (RAT) that infected more than 500,000 computers has pleaded guilty to charges of hacking.

Alex Yücel, 24, faces up to 10 years in prison for his involvement with the $40 program designed to secretly remotely control victims' computers.

The US government says it intends to seize any equipment associated with his nefarious deeds, along with the blackshades.ru and bshades.eu domain names.

The Swedish citizen entered his plea in a Manhattan federal court on Wednesday in response to charges of conspiracy, distribution of malicious software, access device fraud and aggravated identity theft.

His guilty plea was made as part of a deal prior to the commencement of his trial on 22 March this year. After a previous plea deal fell through without explanation, Yücel offered to waive the right to appeal his sentence on condition that it does not exceed 7 years and 3 months in total.

Yücel, who ran the Blackshades organisation under aliases including "Victor Soltan" and "marjinz" was extradited to the US in November 2013 after originally being detained in Moldova.

According to prosecutors, Yücel employed a marketing director and several

customer service representatives to help bolster his business and, by April 2014, the team had generated over $350,000 in sales of the RAT.

Manhattan US Attorney Preet Bharara said:

Through his creation and sale of the Blackshades RAT, Alex Yücel enabled anyone, for just $40, to violate the property and privacy of his victims. With his guilty plea today, Yücel will now have to pay for his conduct. This Office will continue to work with our law enforcement partners at the Federal Bureau of Investigation and around the world to find and prosecute those who create, market, and employ malicious software.

According to documents filed in the Manhattan federal court, the Blackshades RAT - which was used to secretly take nude photos of Miss Teen USA - could give an attacker complete control over an infected system:

Once a computer was infected with the RAT, the user of the RAT had complete control over the computer. The user could, among other things, remotely activate the victim’s web camera. In this way, the user could spy on anyone within view of the victim s webcam inside the victim’s home or in any other private spaces where the victim s computer was used.

The RAT also contained a "keylogger" feature that allowed users to record each key that victims typed on their computer keyboards. To help users steal a victim’s passwords and other log-in credentials, the RAT also had a "form grabber" feature. The "form grabber" automatically captured log-in information that victims entered into "forms" on their infected computers (e.g., log-in screens or order purchase screens for online accounts).

Law enforcement have been keen to crack down on those using, and responsible for, Blackshades.

Over 100 people were arrested in May 2014 in raids associated with Blackshades.

In January 2013, Yücel’s fellow Blackshades creator Michael Hogue pleaded guilty and is still awaiting sentencing.

Blackshades administrator Brendan Johnston appeared in court in November 2014 on charges of conspiracy to commit computer hijacking. His guilty plea could lead to a prison sentence of up to 10 years when he is sentenced on 27 May.

Marlon Rappa, a customer who used the RAT to infect computers, steal personal files and spy on victims via their webcams, pleaded guilty on 31 October 2014. He is due to be sentenced on 13 March.

Most recently, Blackshades customer Kyle Fedorek was yesterday ordered to pay $45,000 in restitution and sentenced to two years in prison, followed by 3 years of supervision, after using the RAT to hack into 90 computers.

Three People Charged over Massive U.S. Email Data Breach

Two Vietnamese citizens and a Canadian have been charged over roles in hacking email service providers in the United States in one of the largest

reported data breaches in the nation’s history, the Department of Justice said on Friday.

Viet Quoc Nguyen, 28, is charged with hacking at least eight email service providers between February 2009 and June 2012 and obtaining more than one billion email addresses.

According to the allegations, Nguyen and fellow Vietnamese citizen Giang Hoang Vu, 25, used the data to send so-called spam to tens of millions of people.

Both men resided in the Netherlands. Vu, who was extradited to the United States in March of last year, pleaded guilty on Thursday to conspiracy to commit computer fraud.

Nguyen remains at large.

The other defendant, Canadian David-Manuel Santos Da Silva, 33, was charged with conspiracy to commit money laundering. He is the co-owner of a company called 21 Celsius Inc, that allegedly struck up a marketing arrangement with Nguyen and Vu to generate revenue and launder the proceeds, according to the Justice Department.

56 Hackers Arrested in Cyber Crime ’Strike Week’ Raids in UK

The United Kingdom’s National Crime Agency (NCA) has arrested 56 suspected hackers in a campaign against cybercrime called "strike week."

Law-enforcement officials conducted, in total, 25 separate operations across England, Scotland and Wales, and those arrested were suspected in a wide range of cyber crimes including:

Network intrusion and data theft from multinational companies and government agencies
Distributed Denial of Service (DDoS) attacks
Cyber-enabled fraud
Malicious software and virus development

The raids conducted by NCA were coordinated by its National Cyber Crime Unit (NCCU), special officers Metropolitan Police and Regional Organised Crime Unit’s (ROCUs), associated with local forces around the UK.

The arrested hackers also include alleged hackers suspected of being behind attacks on Yahoo, the US Department of Defence (DoD), and PlayStation. The list of hackers arrested in the operation is given below:

A 23-year-old man was allegedly responsible for breaching a satellite communications system used by the US Department of Defense. The hacker accessed ’non-confidential contact information’ of almost 800 users, including name, title, e-mail addresses and phone numbers and gained control over information from 34,400 devices, including IMEI numbers.

Another 21-year-old London man was arrested who is suspected of being an alleged member of the D33ds Company hacking collective, the group that hacked into Yahoo in 2012 and posted as many as 450,000 email addresses

and passwords online.

An alleged member of the Lizard Squad, the infamous hacking group which claimed the responsibility for taking down the Xbox Live and PlayStation networks over Christmas, was arrested in Leeds, Yorkshire, BBC reports. Lizard Squad member is believed to be 16-year-old teenager who was also behind the attacks on as many as 350 websites, including Lenovo.

A 20-year-old man from Hackney, London was arrested on suspicion of committing a £15,000 phishing attack.

A 22-year-old was apprehended on suspicion of developing and distributing malware.

Many more suspects were arrested among above; you can read the NCA's full list of arrests here.

"The 56 arrests around the country this week are a result of the essential partnership activity with law enforcement, industry and government that is at the heart of fighting cybercrime," said Andy Archibald, Deputy Director of the NCA's National Cyber Crime Unit.

"Criminals need to realise that committing crime online will not make them anonymous to law enforcement. We are continuously working to track down and apprehend those seeking to utilise computers for criminal ends, and to disrupt the technical networks and infrastructures supporting international cyber crime."

This is't first time when law-enforcement agencies have conducted such massive raids in cyber crimes cases. Last year, the Federal Bureau of Investigation (FBI) also conducted a massive raids in Europe and Australia, and arrested more than 100 customers of Blackshades Remote Administration Tool (RAT) malware.

Blackshades and other malware like it allows hackers to remotely control victims' computers, turning on webcams, stealing usernames and passwords for email and Web services, personal information, and launching further attacks on other computers, without the knowledge of the computer owner.

The malicious program modifies itself in such a way that it evade detection from the computer's antivirus software. Blackshades has been sold via PayPal and underground forums since at least 2010, which cost as little as $40.

However, the recent raids carried out by NCA didn't just target hackers behind well-known attacks or specific cyber crime. Instead it has arrested hackers behind phishing attacks, malware, and also companies that offered web hosting to known criminals.

'Strike week' also suggests that the agencies was monitoring each and every activity of cyber crimes as well as hackers and collecting strong evidences against them. Using that information, the officials raided and arrested a long list of cyber criminals.

Snapchat Tells Teens: Keep Your Clothes On!

Ahh, Valentine's Day: the day of romance, filled as it is with roses,

chocolate, and college kids sneaking into football stadiums to have sex and chronicle it on Snapchat.

Like any Snapchat image that’s timed to disappear within seconds but does not, the image of the young woman in the story above, sans pants, was probably screenshotted before it was posted to a Snapchat account called "Volnationsnaps" and then onto Instagram.

Really, it was just another day for the Snapchat app, where non-disappearing snaps are old hat.

But this time (at least in theory), those kids should have known better, given that Snapchat had launched the Snapchat Safety Center just a few days earlier.

If the football lovers had known (or cared) about Snapchat’s new Safety Center, they would have known that the community guidelines on the new site nix sharing porn or nudes - at least, it does if users are minors.

Snapchat launched the Safety Center on 10 February in conjunction with online safety organisations ConnectSafely, UK Safer Internet Centre, and iKeepSafe.

It’s essentially aimed at parents and teachers of its users, rather than at the users themselves.

In fact, the Safety Center contains a six-page Parents’ Guide to Snapchat that walks worried adults through what the app is, why kids love it, what the minimum age is to use it (13), and what the risks are in using it.

The risks are, of course, that somebody will Snapchat your a**, that snap will be saved by a recipient, and the content will go viral on one of a plethora of venues dedicated to memorialising noteworthy snaps, such as the one taken at the football stadium.

A search on "Snapchat leaked" returns multiple sites devoted to captured snaps of bouncy bits, including an entire Facebook page devoted to the subgenre "College Snapchat Leaked".

From Snapchat’s inception, it was obvious that content could be captured before it disappeared, whether via screenshots, taking a photo of the content with a separate camera, or simply because images that are supposed to disappear forever stay on our mobile phones and on Snapchat’s servers.

Snapchat knows this. To its credit, it’s upfront about it on the new Safety Center.

From the Parents’ Guide:

The ephemeral aspect ... adds a degree of safety, as long as people don’t have a false sense of security about it. Images can be saved as screenshots or captured with another phone and shared without the originator’s knowledge.

If your Snap gets captured by someone you send it to, Snapchat notifies you, but people have found workarounds for that too. So, as always with digital media, 100% safe sharing doesn’t exist.

IAs Snapchat notes, there have been workarounds to evade notification,

such as the one that cropped up when screenshot behaviour in iOS 7 was changed.

Snapchat sure didn’t seem adverse to having its promise of ephemeral content be used by young bodies swapping nude photos, at least in its early days.

As Fusion’s Kashmir Hill points out, the mobile app blatantly pushed its potential for sexting, initially fronting itself with an image of two young girls with a timer placed where their clothes would be.

The community guidelines, along with its stress on not snapping nudies if you’re a minor, aren’t new.

They date to October 2013, appearing six months after nude photos of teen girls at a New Jersey high school were sent through Snapchat and Instagram and then posted by a male recipient.

I doubt that the Safety Center’s emphasis on the guidelines will have much effect on Snapchat users.

Research has shown that sexting and other potentially reputation-damaging content is only exchanged in a small percentage of shared Snapchat content.

But, in spite of a majority (79.4%) of respondents knowing that recovering snaps is possible, a little more than half simply don’t care.

In fact, 52.8% of respondents said that learning about insecure message destruction wouldn’t change their use of the application at all.

But even if user behaviour isn’t likely to change, there’s nothing wrong with trying to inform parents of what dangers their kids are facing with Snapchat.

The new Safety Center is of course a marketing piece as much as anything. But it’s also honest about the risks.

Savvy parents can look beyond the Safety Center’s cheerful graphics, with Snapchat’s happy little cartoon ghosts, playing in their flower-filled playground, and clearly see: this isn’t all jump-rope and picnics.

There be vipers and dragons in these hills.

Burning Man Festival To Cancel Tickets of Cheaters Who Used Website Hacks

Tickets for the annual Burning Man festival in the Nevada desert are hot commodities, with over 80,000 people registering for the recent release of 40,000 tickets.

What started as the burning of a wooden figure on a beach on the summer solstice in 1986 has now grown to a yearly event that attracts tens of thousands of people.

In the last few years, the event has become increasingly popular with the Silcon Valley set, with attendees including Larry Page, Sergey Brin, Elon Musk, Jeff Bezos and Mark Zuckerberg.

Unfortunately for thousands of fans who pre-registered to buy tickets but weren’t able to get through the online queue in time, a flaw in the ticketing website allowed some crafty hackers to game the system in order to jump to the front of the line.

After tickets for the event sold out in an hour last Wednesday, Burning Man acknowledged that some people had cut ahead of others unfairly when the online sale opened.

In a blog post the next day, Burning Man said about 200 people exploited a backdoor in the ticketing website to get to the front of the queue. It assured genuine ticket buyers that the organization was taking steps to address the problem by canceling the fraudulent ticket purchases.

The good news (for us, not them) is that we can track them down, and we re going to cancel their orders. The tickets from those orders will be made available in the OMG Sale in August. Of course, steps are being taken to prevent this from happening again in future sales.

Burning Man organized the online sale as "first come, first served," with a limit of two tickets per person, and required potential buyers to pre-register to receive an email with a link to access the ticketing site.

To manage the online sale of the 40,000 available tickets for the 2015 festival - at $390 a pop - Burning Man used the ticketing agency Ticketfly.

Yet, according to posters at the Burning Man page on Reddit, a few lines of JavaScript embedded in Ticketfly’s online queue revealed the URL of the site’s ’waiting room’, allowing anyone who could read the code to jump ahead.

As reported by Wired, knowing the URL for the waiting room allowed people to purchase tickets ahead of the start of the sale at 12:00 p.m. PST - while everyone else had to wait until the start time and click a button to enter the queue.

The type of flaw that let the cheaters generate the waiting room URL is known as an insecure direct object reference, a coding vulnerability that allows an attacker to bypass authorization and access resources directly by modifying the value of a parameter.

In a similar flaw, Delta Airlines recently emailed flyers URLs to their boarding passes that could be manipulated to gain access to other people’s boarding passes.

E-commerce giant Alibaba made the kind same mistake in its AliExpress online retail portal; and the website for the UK Immobilise National Property Register made a similar snafu.

Java Now Loads Annoying Adware on Macs

Lots of websites require your computer to use the program Java, but the latest update for Macs comes with annoying adware.

The update automatically installs a Web browser add-on for Ask.com. When you perform a search, Ask.com becomes your default option, replacing your preferred search engine (Google, Duck Duck Go, etc.)

Your browser homepage also becomes Ask.com yet another uninvited annoyance.

Previously, only Windows users were subjected to this irritating practice. But now Apple Mac computers celebrated for their clean, simple experience are getting loaded up with the extra, unwanted software too.

There s nothing nefarious about Ask.com on its own. But sneaking in an unnecessary add-on to someone s computer is widely regarded as intrusive. This is the kind of thing that, over time, fills up a computer with undesired software that slows it down. That s why it s often called bloatware.

Oracle, which distributes Java, did not respond to requests for comment on Friday. ZDNet was the first to catch Oracle s new policy.

If you re careful when you update Java, you can avoid downloading the Ask.com bloatware by unchecking the option during the installation process. But the average person who quickly clicks through options will miss it. In that case, users can manually uninstall the software in each browser, and reset the homepage.

Users should have to opt in for extra software. But in this case Oracle is forcing users to opt out.

Companies are often criticized for trying this sort of thing. Major PC manufacturers are notorious for loading bloatware on their laptops at the factory. That s why you get so many pop-ups with stupid programs you never use from Asus, Dell, HP and almost every other computer maker.

Recently, there has been a customer outcry about bloatware. In February, PC maker Lenovo was caught slipping Superfish malware into its laptops and tablets. Superfish is an Internet browser add-on that injects ads onto websites you visit.

Beware! µTorrent Silently Installing Bitcoin Mining Software

If you have recently installed or updated the popular BitTorrent client µTorrent 3.4.2 Build 28913 on your computer, then you read this warning post right now.

Users of the µTorrent file-sharing service are complaining that the latest update of software used for torrent downloading is silently installing a piece of unwanted software called EpicScale, which is basically a Bitcoin mining software.

The Epic Scale, installed without the consent of users, is a cryptocurrency mining software that reportedly uses the combined computing power of users to generate Bitcoin income for BitTorrent company. The unwanted software slows down the host computers and is particularly harder to remove from the system.

The Bitcoin mining software was recently highlighted at uTorrent s

complaint forum where a member Groundrunner says: "There was no information about this during installation and I did opt out of your other bundled software."

A senior manager for customer support at uTorrent did reply to the thread, explaining that the designed the update to ensure partner software downloads don t occur without approval by the user .

"Epic Scale is a great partner for us to continue to generate revenue for the company, while contributing funds to good causes," uTorrent employee wrote. "Feel free to delete this folder. You certainly won t see any persistent auto-reinstalls of the software, it will be gone from your machine for good."

The troubling part of Epic Scale is that it can t be uninstalled by simply following the regular uninstallation procedure on Window machines, whereas uTorrent employee described Epic Scale as "easy to uninstall".

Okay! Let s agree that Epic Scale is used by uTorrent to generate revenue, but bundling the application with uTorrent is highly problematic to the normal user as it will consume system resources all the time while running. A users complaint that the software is "easily noticeable by the increased CPU load when the computer is idle."

The silent install appears to happen selectively, and not on all machines. BitTorrent spokesperson said, "We have reviewed the issue closely and can confirm there is no silent install happening. We are continuing to look at the issue."

Users that don’t notice the program may find significantly decreased performance as a result. Windows users are recommended to check the Task Manager (Ctrl-Shift-Esc) to make sure EpicScale is not running on their system.

So far, uTorrent is the most visited BitTorrent client worldwide with more than 150 Million active users every month. So one can imagine, if 10% of them have upgraded their software to the latest malicious version, then how much revenue company could have generated by burning their CPUs within one day.

If you think that it s time to move on to other Torrent downloads, meanwhile, you can try Deluge, Vuze, Bitcomment, qBittorrent which are lightweight, free, cross-platform torrent clients available for Linux, Mac OS X and Windows.

Whether its a software, or an online service, you have to agree to a so-called End User License Agreement. They are so common, in software and on the Internet, that many users ignore them and blindly click "Agree" without understanding what they’re agreeing to.

An average user spent only 6 seconds on every page while installing a Software, Next... Next... Install... and Finish.

In the below screenshot you can read, µTorrent software is giving an option to "Accept" or "Decline" the offer, but they have described "Epic Scale" as a ’distributed computing platform’ that perform ’computation’ only and asking users to ’Join us to help support organisation working to cure AIDS’ by donating our system resources.

It is clear that an average user will never understand that they are

allowing it to install a ’Bitcoin Mining Software’, which is used to generate revenue by consuming their system resources massively.

So either the users are collectively mistaken or there is a lack of transparency in the software installation, leading to confusion amongst users.

Apple Releases Public Beta of Mac OS X 10.10.3 with New Photos App

Apple s just released the first beta of OS X 10.10.3, which includes the company s all new Photos app, for participants of its public beta program. If you were previously signed up to receive early access to OS X Yosemite ahead of its September launch, you should be able to download this 10.10.3 update by opening the Mac App Store and clicking the updates tab.

If not, you can still head to Apple s website and sign up for beta downloads. The process is pretty simple and basically involves just two steps: register your Apple ID, and then download a small file that authorizes your Mac to receive the early software. Of course, you should definitely back up your computer before installing the beta should anything go awry; there s no simple way of downgrading back down to 10.10.2. And it s really only advisable to install this update on a secondary Mac you ve got sitting around using beta software on your primary machine is a risky move.

But if you re dying for a chance to try out the new, pretty great Photos app before everyone else, this is your opportunity. Even if the software s not final, this early peek should help you decide if you re ready to trash iPhoto and Aperture and stick with Apple s new app. What Apple already s got here the improved cloud syncing and far speedier performance, especially is worth getting excited about. Before you dive into the beta, here s everything you need to know about Photos. OS X 10.10.3 also includes new emoji and easier logins for Google users who take advantage of two-step verification.

How To Test Apple’s New Photos App for Mac

Apple has released the public beta of its Photos app for OS X. We detail where you sign up to put the new app through its paces.

Last month, Apple raised the curtain on its new Photos app for OS X. Our Jason Parker took it for a spin and found it to bring a level of simplicity more commonly found on iOS to Apple’s desktop platform OS X. Since that time, Photos has been in a somewhat private beta wherein only registered developers had access to OS X Yosemite 10.10.3, which includes the new applications.

Apple had promised a public beta for everyday users to test, experiment and report any bugs found in the app back to the Cupertino-based company. And today, Apple made good on that promise by releasing a public beta for OS X 10.10.3.

If you had signed up to test OS X Yosemite last summer, you should still

be enrolled in the program. If so, an update will be available for you in the Mac App Store under the Updates tab.

For those who never registered for the original Yosemite beta, you can still sign up. You'll need to visit Apple's OS X Beta Program site and sign up using your Apple ID.

During the signup process, you're reminded to create a backup of your Mac using Time Machine (or the like) and are walked through potential pitfalls of using beta software.

Once you agree to the terms of the beta, you need to download and install a small program that registers your Mac with the beta program. From there, all future updates are done through the Mac App Store.

The entire process from signing up until you have 10.10.3 installed will vary depending on your connection speed and Mac, but I'd suggest setting aside an hour for the initial installation of the beta. You'll need even more time if you've yet to back up your Mac.

With New Office 2016 Preview, Microsoft Brings Mac Users into the Modern Era

Microsoft has released the first public preview of Office 2016 for Mac, its updated Office suite for Mac OS 10.10 users, which is due out this summer.

I've had a few days to try out the new Office apps ahead of their public release. Here's what you can expect.

The preview consists of three new apps - Word, Excel, and PowerPoint - plus updates to the Outlook and OneNote apps that were already available as previews. On my Mac, the new apps run side by side with Office for Mac 2011, making it easy to compare old and new.

For Mac users, the new user interface is a radical (and long-overdue) refresh of the classic Office look and feel.

In Office for Mac 2011, the mix of toolbars, menus, and ribbons is downright ugly. The revised design closely resembles Office 2013 for Windows, with Save, Open, Undo, and Redo buttons alongside the window controls in the title bar; all other commands are clustered in a single ribbon that can be collapsed for a clutter-free experience. Compare the clean new look (top) with the old, messy Office 2011 design.

If you've used Office 2013 on a Windows PC, the experience of switching to the new Mac version will feel very familiar, Microsoft is trying with this release to unify the interface across multiple platforms.

That means task panes for common formatting tasks, like this list of Styles in Word.

In addition, the experience of creating a chart in Excel is nearly identical in Office 2016 on the Mac as it is in Office 2013 for Windows. Overall, it's an enormous improvement over the kludgey mess of buttons and menus in Office 2011.

Unsurprisingly, the new Office for Macs continues Microsoft's relentless

push toward the cloud. To open or save a file, you'll use the Mac version of Backstage view. OneDrive and OneDrive for Business locations are at the top of this list, although you can still override cloud storage and save files locally using the On My Mac shortcut.

One feature that Mac users get ahead of their Windows counterparts is visible in the above screen. Opening a OneDrive folder shows files stored in your own OneDrive account but also shows OneDrive folders and files shared with you by other users.

There are also additional collaborative features, including threaded comments for Word documents.

In general, as a longtime Office for Windows user I found the three new apps in the Mac suite to be sufficiently feature-rich for productive use. The one app where I felt short-changed when switching to the Mac is Outlook, which is considerably simpler than its Windows counterpart.

The latest preview release of Outlook 2016 for the Mac has a few nice features, including conversation view and the ability to review drafts and junk mail for multiple accounts in a single location.

Outlook 2016 for the Mac supports Outlook.com (Hotmail) accounts in IMAP mode only. It also supports Gmail, iCloud, and Exchange-based accounts, including Office 365. One feature I desperately missed from Outlook 2013 for Windows is the ability to specify that I only want to sync a limited selection of messages for a specific account.

Overall, this is a very promising preview. If you use Office on the Mac, and especially if you have an active Office 365 subscription, it's well worth the download.

Facebook Comes Up with New Ways To Reach Out to the Suicidal

"I am thinking of jumping", the Facebook post said.

Attached to the post were pictures of the George Washington Bridge to Manhattan.

An alarmed friend of the 18-year-old contacted authorities. Port Authority Police Department Lt. Thomas Michaels, assigned to the bridge, responded by reaching out to the cyberbullied teen with his own Facebook message.

In the post, Lt. Michaels included his phone number, along with a plea for the teen to call.

Eventually, the troubled teen did. He agreed to meet with Michaels and to then be taken to hospital for help.

Unfortunately, not all suicidal notes that get posted to Facebook - or to other social media sites, such as Amanda Todd's final YouTube post or Leelah Alcorn's heartbreaking Tumblr goodbye - have happy endings.

Now, Facebook has stepped up to help both those experiencing suicidal inclinations and the frantic friends who spot their messages.

On Wednesday, Facebook announced new and improved tools to help prevent suicide, providing resources, advice and support not only for troubled users but for those reporting them.

The network worked with the mental health organizations Forefront, Now Matters Now, the National Suicide Prevention Lifeline, Save.org and others on the updates, as well as consulting with people who've experienced self-injury or suicide.

It turns out that a social network such as Facebook can be a vital way to reach suicidal people, given that, as experts told Facebook, connecting with people who care can help those in distress.

The first thing Facebook asks when users report a direct threat of suicide is that they contact local emergency services immediately.

It also asks users to report troubling content so that its teams - which work around the world, 24/7 - can review it. These teams prioritize self-injury reports and send help and resources to those in distress.

Now, Facebook said in a post on Wednesday, it's offering them more support:

We have significantly expanded the support and resources that are available to them the next time they log on to Facebook after we review a report of something they ve posted. Besides encouraging them to connect with a mental health expert at the National Suicide Prevention Lifeline, we now also give them the option of reaching out to a friend, and provide tips and advice on how they can work through these feelings.

Facebook is also offering help to whomever flags a troubling post, including the option of calling or messaging the friend whom they're worried about, to let them know that somebody cares, or to reach out to other friends or trained suicide hotline professionals.

The company's doing this because it's the most important work Facebook has, it says:

Keeping you safe is our most important responsibility on Facebook.

The changes will roll out in the US in the coming months, with improved tools now being worked on for those outside of the US.

Hopefully, Facebook's commendable efforts will help people who don't know where to turn when they're suffering from suicidal thoughts or when they see such thoughts coming through from others on their newsfeeds.

Let's hope that Facebook's work inspires all social media venues to follow suit. This is work profoundly worthy of emulating.

Kudos, Facebook.

Twitter Troll Fired, Another Suspended After Curt Schilling Names and Shames The m

You know that old advice about dealing with trolls by ignoring them, instead of feeding them the attention they want?

Former Red Sox pitcher Curt Schilling doesn’t, apparently.

Instead, this is his strategy in the first inning of a game called mess with my daughter and I’ll knock you clear out of the ballpark: naming and shaming on his blog.

This is how it started: last week, Schilling - a professional ball player for 22 years - proudly tweeted his congratulations to his daughter, 17-year-old Gabby Schilling, who’d been accepted to Salve Regina University, where she’ll play softball.

Congrats to Gabby Schilling who will pitch for the Salve Regina Seahawks next year!!

A variety of responses came in.

The first batch were predictable, with responses like "Can t wait to date her!"

Then came some schoolboy nastiness, and it spiraled down from there - with mentions of rape and other vulgar acts, in one of those one-upmanship troll contests that are so miserably common on Twitter.

The contest also sprawled into personal tweets, texts and email to "more than one party," Schilling says.

A father’s vengeance when his daughter is threatened is a mighty thing.

The protective father in this case had, within 1 hour, tracked down the names and schools of the antagonists, as well as the sports and playing positions of 7 trolling athletes.

Schilling told the NY Daily News that so far, he’s aware of nine trolls who’ve been fired or kicked off athletic teams because of his having published their tweets - "and we re not done."

He went into detail about two of the worst, including their names and backgrounds.

One of them, identified by Schilling as a recent graduate of Montclair (New Jersey) State University, was fired by the Yankees as a part-time ticket seller on Monday after the team learned of his posts.

Schilling identified another troll as a Brookdale Community College student.

Avis McMillon, a spokeswoman for the New Jersey school, told the newspaper that the student has been summarily suspended:

The student has been summarily suspended and will be scheduled for a conduct hearing where further disciplinary action will be taken.

Both the trolls’ Twitter accounts have been deactivated, and their tweets have been deleted.

Schilling has no sympathy for them, even after the trolls turned apologetic:

I found it rather funny at how quickly tone changed when I heard via email

from a few athletes who d been suspended by their coaches. Gone was the tough guy tweeter, replaced by the ’I m so sorry’ apology used by those only sorry because they got caught.

A mistake is tweeting once and saying ’damn, I’m an idiot’ and taking it down. These guys? They’re making conscious choices to cyberbully an amazing and beautiful young woman on the internet, that none of them know by the way, because they don’t like her dad or they somehow think saying words you can teach a 5 year old is tough?

Predictably enough, some of the trolls’ friends told Schilling to "lighten up", given that their buddies were "just joking."

Why, they asked, would Schilling say things that might "ruin someone s life ?

Schilling’s response was apt, and it was chilling: he listed links to news articles about dozens of cyberbullying-prompted suicides, including that of 12-year-old Rebecca Ann Sedwick, 15-year-old Amanda Todd and many other teens who were taunted on Ask.fm.

He also reminded the trolls - and everyone else who uses the internet - just what happens when you say or do something online:

What these kids are failing to realize, what this generation fails to realize is this; Everything they ve just said and done? That is out there now, forever. It can, and in some cases will, follow them for the rest of their lives.

Schilling told CBS News that he’s been contacted by the FBI and two local police departments, and is discussing filing possible criminal charges.

Facebook Post Criticizing Employer Lands Florida Man in Abu Dhabi Prison

Bad things happen when we publicly post things that upset our bosses.

Sometimes, posts result in getting fired.

Sometimes, posts lead to losing a job before it starts.

But for a Florida man who posted about the company he worked for in the United Arab Emirates, the outcome was far more severe: it resulted in getting tossed into a Middle Eastern jail.

The Associated Press reports that Ryan Pate, a helicopter mechanic from Belleair Bluffs, Florida, had a mixup over sick leave with the company he was working for, Global Aerospace Logistics.

Pate, 30, told the AP that he had traveled home to Florida in December to spend the holidays with his family and to propose to his girlfriend, Jillian Cardoza.
He was also hoping, while in Florida, to get treatment for a back injury.

But seeing a doctor would have meant extending his leave, and that’s where the disagreement boiled up.

After one particularly thorny phone call, Pate took to Facebook to

complain about Global Aerospace Logistics.

Pate can’t remember exactly what he wrote. He does remember throwing the word "backstabbers" into the post, which warned other contractors not to work for his employer.

Then, without giving it much further thought, he returned to Abu Dhabi to file paperwork required to end his employment, to empty out his apartment, and to sell his car.

Soon after he arrived, he got a call from the police, telling him to come to the station. That’s when police showed him screenshots of his comments.

Officers arrested Pate for breaking an Emirates law against slandering his employer.

Cardoza said Pate sent her this text from the station:

I’m being arrested. I’m so sorry. I love you.

Pate spent about 10 days in jail. As of Thursday, he was free on bail, awaiting his trial on 17 March.

If convicted, he’s facing up to five years in prison and a steep fine.

Pate’s congressman, Rep. David Jolly, is working on his constituent’s behalf, lobbying the State Department and Emirates officials for help.

Jolly has written to the Emirati attorney general, pointing out (respectfully) that, since the posts occurred while Pate was on US soil, the Emirati laws shouldn’t apply.

A State Department spokeswoman, Marie Harf, told the AP that a consular officer had visited Pate in prison and that the embassy in Abu Dhabi would continue providing assistance.

In a phone interview with the AP, Pate said he’s so accustomed to First Amendment protection of free speech that he never imagined his post could lead to such a serious outcome:

I just couldn’t register it in my head because as an American growing up in the United States, the First Amendment right is just ingrained in my brain. I never even entertained the fact that I would wind up in prison out here for something I put on Facebook in the United States.

He also said that he’s remorseful for letting his emotions get the better of him.

Pate certainly isn’t the first to suffer the consequences of unwise postings.

A high-profile case of people who’ve had their careers shoved into the mud came up earlier this week when Curt Schilling named and shamed Twitter trolls, leading to nine trolls who’ve been fired or kicked off athletic teams.

But while Pate isn’t the first to regret a post, his is one of the most egregious outcomes.

To paraphrase Schilling, in the real world, you get held accountable for the things you say.

If you're not careful, accountability can be severe, whether it's getting fired, getting suspended from college, or even imprisonment.

Please learn from Pate's example, and don't forget: the First Amendment, or whatever law protects free speech in your own country, stops at the borders.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.